WHAT IS CLAIMED IS:

1. A method of securing content stored on media, the method comprising:
attaching content privileges to the media, wherein the privileges govern a plurality of levels of access; and
configuring the media to permit access to the content according to the content privileges and predetermined conditions.

2. The method of claim 1 wherein one of the levels of access to the content includes at least one of playback, copying and manipulating of the content.

3. The method of claim 2 wherein the copying of content includes copying one of a limited number and an unlimited number of copies of pre-recorded content.

4. The method of claim 3 wherein the unlimited number of copies relates to one of an original source of the content being copied and a copied original source of the content being copied.

5. The method of claim 1 wherein the predetermined conditions include one or more of:
authenticating a channel for delivery of the content; and
checking a revocation list for a revoked indicator before permitting access, wherein presence of the revoked indicator precludes permitting access.

6. The method of claim 1 wherein the attached content privileges operate with a data management system wherein the content is stored on the media, the management system managing access to the content.

7. The method of claim 6 wherein the data management system includes firmware located in a controller, the firmware including at least a secure application programming interface (API) and an open API, wherein:
the open API allows access to file system data on the media; and
the secure API allows access to secure data on the media according to one or more identifiers on the media.

8. The method of claim 7 wherein the secure API includes a first secure API and one or more additional secure APIs, the first secure API operable with the one or more additional secure APIs, the one or more additional secure APIs providing additive layers of security, the first secure API controlling access to the content with the additive layers of security.

9. The method of claim 7 wherein the firmware is included on an application specific integrated circuit (ASIC).

10. The method of claim 6 wherein the data management system manages content access via at least one application programming interface (API), the API restricting access to the media by a host.

11. The method of claim 10 wherein the API is capable of preventing block level access to the content.

12. The method of claim 10 wherein the API is accessible only via an authenticated channel.

13. The method of claim 1 wherein the media is portable media, including an optical disk and the content includes one or more of mastered content, recorded content, copied content and unlocked content and locked content.

14. The method of claim 7 wherein the identifier provides a seed for a key box, the key box providing keys for at least one of unlocking data and decrypting content.

15. The method of claim 14 wherein the media holds one or more of mastered content and recorded content, the mastered content and the recorded content each being associated with a key box, the key box being bound to the media.

16. The method of claim 15 wherein the mastered content and the recorded content, together with their associated key boxes each provide a complete accessing system.

17. The method of claim 15 wherein the key box may be unbound from a first media and rebound to a second media to create a to a complete accessing system on the second media with the key box bound thereto.

18. An apparatus for securing content stored on media, the apparatus comprising:
at least one tool for transferring content onto the media, the tool configured to attach a plurality of levels of access, wherein content privileges and predetermined conditions govern access to the content.

19. The apparatus of claim 18, further comprising:
a dongle coupled to the tool, the dongle configured to bind a key box to the media.

20. The apparatus of claim 19 further comprising:
an application specific integrated circuit (ASIC) coupled to the dongle, and
a random key generator embedded with the ASIC, the random key generator providing at least one secret key for the media.

21. The apparatus of claim 18 wherein the content privileges include at least one or more of playback, copying and manipulating of the content.

22. The apparatus of claim 21 wherein the content privilege of copying of content includes copying a limited number of copies of specified content.

23. The apparatus of claim 18 wherein the predetermined conditions include one or more of:
authenticating a channel for delivery of the content; and
checking a revocation list for a revoked indicator before permitting access, wherein presence of the revoked indicator precludes permitting access.

24. The apparatus of claim 18 wherein the attached content privileges operate with a data management system wherein the content is stored as block data on the media, the management system managing the block data via firmware on the application specific integrated circuit (ASIC) that prevents access to the content outside of the firmware.

25. The apparatus of claim 24 wherein the ASIC is located in a controller, the firmware on the ASIC including at least a secure application programming interface (API) and an open API, wherein:

the open API allows access to file system data on the media; and

the secure API allows access to secure data on the media according to one or more identifiers on the media.

26. The apparatus of claim 25 wherein the secure API includes a first secure API and one or more additional secure APIs, the first secure API operable with the one or more additional secure APIs, the one or more additional secure APIs providing additive layers of security, the first secure API controlling access to the content with the additive layers of security.

27. The apparatus of claim 24 wherein the firmware manages content access via at least one application programming interface (API), the API preventing block level access to the media by a host.

28. The apparatus of claim 27 wherein the API prevents block level access to the content via a host.

29. The apparatus of claim 27 wherein the API is accessible only via an authenticated channel.

30. The apparatus of claim 18 wherein the media is portable media, including an optical disk and the content includes one or more of mastered content, recorded content, copied content and unlocked content and locked content.

31. The apparatus of claim 25 wherein the identifier provides a seed for a key box, the key box providing keys for at least one of unlocking and decrypting data.

32. The apparatus of claim 31 wherein the media holds one of mastered and recorded content, the mastered and recorded content together with their associated key boxes each providing a complete accessing system.

33. The method of claim 31 wherein the key box may be unbound from a first media and rebound to a second media to create a to a complete accessing system on the second media with the key box bound thereto.

34. A method for mastering secure pre-recorded content comprising:

encrypting the pre-recorded content; and

binding a key box and one or more identifiers to a media disk, the key box configured to use the identifier with the key box, wherein the identifiers include one or more of a complete identifier and a partial identifier, the partial identifier requiring completion via a secondary transaction prior to using the key box.

35. The method of claim 34 wherein the key box is configured to provide keys for operating a triple-DES block, the triple-DES block receiving an output of a random key generator, the random key generator being seeded by the completed identifier from the media disk, the triple-DES block using the completed identifier with the key box for decrypting and encrypting the content.

36. The method of claim 34 wherein the identifiers include public and private identifiers.